Configuring and Troubleshooting an ATA 186 with Cisco IOS Gatekeepers

Document ID: 19084

Introduction

The Cisco Analog Telephone Adaptor (ATA) 186 is a handset–to–Ethernet adaptor that interfaces regular analog phones with IP–based telephony networks. The ATA 186 has two voice ports that can only support legacy analog touch tone telephones. Unlike the regular Foreign Exchange Station (FXS) ports, these can not be interfaced with a private branch exchange (PBX) because the ATA 186 can not send out digits on these ports. With this configuration, you can use both voice ports with different E.164 addresses on each.

Prerequisites

Requirements

This document assumes that the reader is familiar with the content in the Cisco ATA 186 Basic Configuration document.

This configuration requires ATA 186 to be at version 2.0 or later, using the H.323 feature set.

Ensure that there is IP connectivity between the ATA 186, gateway, and gatekeeper devices. Also, ensure that the ATA 186 is accessible through the web server method for further configuration.

Components Used

The information in this document is based on these software and hardware versions:

- ATA 186 with version 2.12
- Cisco 3640 with Cisco IOS® Software Release 12.1 as a gateway
- Cisco 2600 with Cisco IOS Software Release 12.2 as a gatekeeper

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Network Diagram

This document uses this network setup:
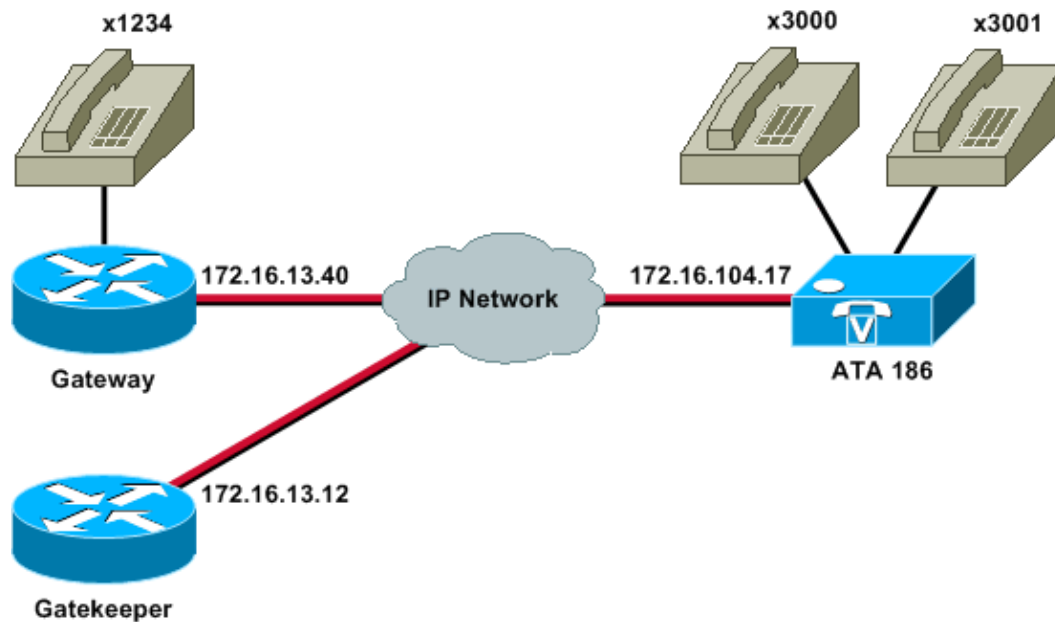
Registering the ATA 186 with the Gatekeeper

Follow these instructions to register the ATA 186 with the gatekeeper.

1. In a web browser Address or Location field, type the URL **http://*ip_address_of_ata*/dev** to access the ATA 186 configuration screen, where *ip_address_of_ata* is the IP address of the ATA 186 you are registering.

   In this example, the URL is http://172.16.104.117/dev. The Cisco ATA 186 Configuration window appears.

   Note: The underlined fields are the relevant configured parameters for this scenario.

Cisco ATA 186 Configuration
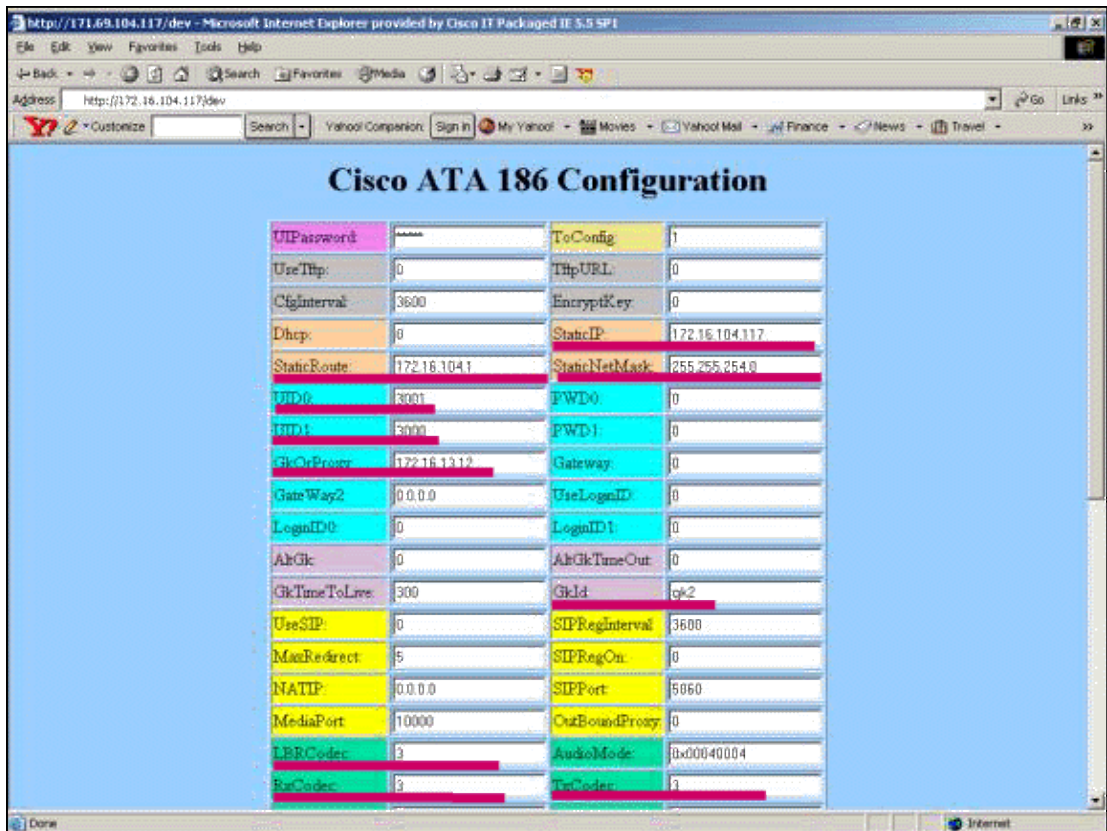
IP addressing can be done statically or dynamically, as explained in the Cisco ATA 186 Basic Configuration document. In the previous screen, the static IP address is used.

2. In the Cisco ATA 186 Configuration window, configure these fields:

♦ UID0 and UID1 Configure the E.164 addresses of voice ports 0 and 1.

Both voice ports can not have the same E.164 address, as the ATA 186 can not hunt if one of the ports is busy. If both voice ports are assigned the same E.164 address, the call will always be sent to the first voice port. If this port is busy, the busy signal is sent to the caller.

♦ RxCodec and TxCodec Configure the codec ID.

◊ G.723.1 codec ID 0.
◊ G.711a codec ID 1.
◊ G.711u codec ID 2.
◊ G.729a codec ID 3.

In the configuration shown below, the G.729r8 codec is used on the ATA 186 *and* on the gateway.

♦ LBRCodec Configure as 0 or 3, based on the chosen codec.

◊ LBRC is 0 G.723.1 codec is available to both FXS ports at any time. Each line can maintain two G.723.1 calls in a non−conference state. Therefore, up to four G.723.1 calls can be maintained in the Cisco ATA 186. An example is call waiting.
◊ LBRC is 3 G.729a is available to one of the two FXS ports on a first−come−first−served basis. If the Cisco IOS gateway is configured with the default G.729 codec, only one ATA 186 port can be used. To prevent the second call from failing, configure a voice codec−class on the gateway to negotiate the second call using a G.711 codec. For detailed information, refer to the Codec Negotiation section of the Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation document.

◆ GKOrProxy Configure the IP address of the gatekeeper.

Once this is done, anything that is dialed from the ATA 186 voice ports is sent to the gatekeeper.

3. Click the **Apply** button and then reload the page.

The ATA 186 takes 10 seconds to reconfigure itself.

These examples are relevant configurations for the Cisco IOS gatekeeper and gateway:

2610–Gatekeeper

```
interface Ethernet0/0
 ip addreinterface Ethernet0/0
 ip address 172.16.13.12 255.255.255.224
 half-duplex
 h323 interface
 h323 h323-id pro
 h323 gatekeeper ipaddr 172.16.13.12
 h323 t120 bypass
!
dial-peer cor custom
!
!
!
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
no shutdown
!
```

3640–Gateway

```
interface Ethernet0/0
 ip address 172.16.13.40 255.255.255.224
 half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.13.33
ip http server
!
!
!
voice-port 3/0/0
!
voice-port 3/0/1
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 destination-pattern 34
 port 3/0/0
!
dial-peer voice 2 pots
 destination-pattern 45
 port 3/0/1
!
dial-peer voice 100 pots
 destination-pattern 1234
 port 3/0/0
!
dial-peer voice 3000 voip
```

```
   destination-pattern 300.
   session target ras

!--- Dial-peer to send the calls to ATA.

!
```

Adding Security

As of ATA software release 2.12, the options in this section are available to add security.

Authenticate the Endpoint at the Gatekeeper with an H.323 ID

Follow these steps to configure the ATA 186 to register with the H.323 ID:

1. Set the AutMethod field to **0** (the default is 1).

   The hexadecimal value that is to be configured for this field is 0x0.
2. Set the UseLoginID field to **1**.
3. Configure LoginID0 and LoginID1, with the H.323 IDs for the ATA 186.

   The ATA 186 registers as two different H.323 terminals, one for each port.

This is a sample working configuration for the gatekeeper when using ATA with the H.323 ID authentication method:

2610–Gatekeeper

```
aaa authentication login default local
aaa authentication login cisco none
```

```
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username atagw1

!--- Same as the LoginID0 and LoginID1 fields.

username atagw2
username 3640

!--- Same as the H.323 ID configured on the gateway.

!
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
security any

!--- Register after the H.323 ID or E.164 address is authenticated.

no shutdown
!
```

Authenticate the Endpoint at the Gatekeeper with an E.164 Address

Follow these steps to configure the ATA 186 to register with the E.164 address:

1. Set the AutMethod field to **0** (the default is 1).

   The hexadecimal value that is to be configured for this field is 0x0.
2. Set the UseLoginID field to **0**.

   The ATA uses the UID0 and UID1 fields to get authenticated by the gatekeeper.

This is a sample working configuration for the gatekeeper and gateway when using ATA with the E.164 ID authentication method:

2610–Gatekeeper

<pre>aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username 3001
 	
!--- Same as the UID0.
 	
username 3000
 	
!--- Same as the UID1.
 	
!
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
security any
 	
!--- Register after the H.323 ID or E.164 address is authenticated.
 	
no shutdown
!</pre>

Authenticate the Endpoint at the Gatekeeper with an H.323 ID and Password

Follow these steps to configure the ATA 186 to register with the H.323 ID and password:

1. Set the AutMethod field to **1** (the default is 1).

   The hexadecimal value that is to be configured for this field is 0x1. This field is set to indicate that the ATA now looks for the password.
2. Set the UseLoginID field to **1**.
3. Configure LoginID0 and LoginID1, with the H.323 IDs for the ATA 186.

   The ATA 186 registers as two different H.323 terminals, one for each port.
4. Configure PWD0 and PWD1 with the password for each port.

   Note: The ATA uses the password to generate the token. This token is sent to the gatekeeper for authentication.
5. Configure NTPIP with the Network Time Protocol (NTP) server s IP address.

   The gatekeeper and the ATA must have clocks synchronized to the same NTP server.

Note: The timestamp is used for token generation. For more information, refer to the Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide.

This is a sample working configuration for the gatekeeper and gateway when using ATA with the H.323 ID and password authentication method:

2610–Gatekeeper

```
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username atagw1 password cisco

!--- Same as the LoginID0 and PWD0 fields.

username atagw2 password cisco

!--- Same as the LoginID1 and PWD1 fields.

!
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
security token required-for registration

!--- Register after the H.323 ID or E.164 address and token is authenticated.

no shutdown
!
```

Note: For more information on gatekeeper security, refer to the Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide.

Authenticate the Endpoint at the Gatekeeper with an E.164 Address and Password

Follow these steps to configure the ATA 186 to register with the E.164 ID and password:

1. Set the AutMethod field to **1** (the default is 1).

   The hexadecimal value that is to be configured for this field is 0x0. This field is set to indicate that the ATA will now look for the password.
2. Set the UseLoginID field to **0**.
3. Configure UID0 and UID1 with the E.164 IDs for the ATA 186.

   The ATA 186 registers as two different H.323 terminals, one for each port.
4. Configure PWD0 and PWD1 with the password for the each port.

   Note: The ATA uses the password to generate the token. This token is sent to the gatekeeper for authentication.
5. Configure NTPIP with the NTP server s IP address.

   The gatekeeper and the ATA must have clocks synchronized to the same NTP server.

Note: The timestamp is used for token generation. For more information, refer to the Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide.

This is a sample working configuration for the gatekeeper and gateway when using ATA with the E.164 ID and password authentication method:

```
                              2610–Gatekeeper
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username 3001 password cisco

!--- Same as the UID0 and PWD0 fields.

username 3000 password cisco


!--- Same as the UID1 and PWD1 fields.

!
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
security token required-for registration

!--- Register after the H.323 ID or E.164 address and token is authenticated.

no shutdown
!
```

Note: For more information on gatekeeper security, refer to the Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide.

Authenticate the Endpoint at the Gatekeeper with an H.323 ID and Password Using the Separator

Follow these steps to configure the ATA 186 to register with the H.323 ID and password:

1. Set the AutMethod field to **1** (the default is 1).

   The hexadecimal value configured for this field is 0x1. This field is set to indicate that the ATA now looks for the password.
2. Set the UseLoginID field to **1**.
3. Configure LoginID0 and LoginID1 with the H.323 IDs, followed by the separator and password for the ATA 186.

   For example, LoginID0 is **atagw1=cisco**.

   The ATA 186 registers as two different H.323 terminals, one for each port.

   Note: The ATA uses the password to generate the token. This token is sent to the gatekeeper for authentication.
4. Configure NTPIP with the NTP server s IP address.

   The gatekeeper and the ATA must have clocks synchronized to the same NTP server.

Note: The timestamp is used for token generation. For more information, refer to the Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide.

This is a sample working configuration for the gatekeeper and gateway when using ATA with the H.323 ID and password authentication method using a separator:

2610–Gatekeeper
<pre>aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username atagw1 password cisco

<i>!--- Same as the LoginID0 and PWD0 fields.</i>

username atagw2 password cisco

<i>!--- Same as the LoginID1 and PWD1 fields.</i>

!
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
security h323-id
security password separator =

<i>!--- Register after the H.323 ID or E.164 address and token is authenticated.</i>

no shutdown
!</pre> |

Note: For more information on gatekeeper security, refer to the Gateway to Gatekeeper (H.235) and Gatekeeper to Gatekeeper (IZCT) Security Troubleshooting Guide.

Verify

The example in this section shows the gatekeeper endpoint registration.

To verify the configuration, issue the **show gatekeeper endpoint** command.

```
                          GATEKEEPER ENDPOINT
    REGISTRATION

    CallSignalAddr   Port   RASSignalAddr   Port   Zone Name   Type      Flags
    --------------   ----   -------------   ----   ---------   ----      -----
    172.16.13.40     1720   172.16.13.40    50923    gk2       VOIP-GW   E164-ID: 1234
                                                                        H323-ID: 3640
    172.16.13.43     1720   172.16.13.43    58400    gk2       VOIP-GW   H323-ID: 3660-2
    172.16.104.117   1720   172.69.85.90    1719     gk2       TERM      E164-ID: 3000
    172.16.104.117   1721   172.69.85.90    1739     gk2       TERM      E164-ID: 3001
    Total number of active registrations=3
```

Note: The ATA 186 registers as an H.323 terminal (`TERM`) and not as an H.323 gateway. This is done deliberately so that only the calls intended for the ATA 186 are sent to it.

Note: You can not have any address in the ATA gateway field. You can not configure the ATA 186 to work with the gatekeeper as well as the gateway.

Troubleshoot

This section provides information to troubleshoot your configuration.

The ATA 186 does not provide dial tone if it is not successfully registered with the gatekeeper. If the ATA 186 is not registering with the gatekeeper, verify these items:

- IP connectivity exists between the ATA 186 and the gatekeeper.
- The ATA 186 UID0 and UID1 fields are configured correctly.

    ♦ If the UID fields are set to 0, the ATA 186 does not attempt to register with the gatekeeper.
    ♦ At the least, the UID0 field must be a non−zero value, for the ATA 186 to start the registration process.
    ♦ If both ATA 186 ports (UID0 and UID1) have non−zero E.164 addresses, the ATA 186 attempts to register with both ports. The ATA 186 does not provide dial tone, even if one of the ports is unable to register.
- The gatekeeper is configured correctly.

    ♦ If the gatekeeper is configured with a local zone prefix, the E.164 address of the ATA 186 must be included.
    ♦ If security is configured on the gatekeeper, the ATA 186 must be configured accordingly.

In addition, verify that the UseSIP field is set to 0. This is necessary to configure the ATA 186 in H.323 mode. If the UseSIP field is set to 1, the ATA 186 does not send the registration request to the gatekeeper.

Troubleshoot the Gatekeeper

When security is configured, issue the **debug aaa authentication** command.

If no security is configured, issue the **debug ras** command.

Note: The ATA 186 registers for the two voice ports separately. The ATA 186, therefore, gets authenticated twice as different H.323 terminals, as shown in this debug:

```
4w4d: AAA/AUTHEN/CONT (3800768902): continue_login (user='atagw1')
4w4d: AAA/AUTHEN (3800768902): status = GETPASS
4w4d: AAA/AUTHEN/CONT (3800768902): Method=LOCAL
4w4d: AAA/AUTHEN (3800768902): status = PASS
4w4d: AAA: parse name=<no string> idb type=-1    tty=-1
4w4d: AAA/MEMORY: create_user (0x83149EFC) user='atagw2'ruser='NULL' port='NULL'
       rem_addr='NULL' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0'
4w4d: AAA/AUTHEN/START (294225678): port='' list='h323' action=LOGIN service=LOGIN
4w4d: AAA/AUTHEN/START (294225678): found list h323
4w4d: AAA/AUTHEN/START (294225678): Method=LOCAL
4w4d: AAA/AUTHEN (294225678): status = GETPASS
4w4d: AAA/H323: Password:
4w4d: AAA/AUTHEN/CONT (294225678): continue_login (user='atagw2')
4w4d: AAA/AUTHEN (294225678): status = GETPASS
4w4d: AAA/AUTHEN/CONT (294225678): Method=LOCAL
4w4d: AAA/AUTHEN (294225678): status = PASS
4w4d: AAA: parse name=<no string> idb type=-1    tty=-1
4w4d: AAA/MEMORY: create_user (0x831910C0) user='3660'  ruser='NULL' port='NULL'
       rem_addr='NULL' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0
```

For more troubleshooting examples, refer to Troubleshooting Gatekeeper Registration Issues.

Troubleshoot the ATA 186

When you are working with third−party gatekeepers and gateways, the troubleshooting tool on the ATA 186 is very helpful. To enable the ATA 186 troubleshooting tool, follow these steps:

1. In the ATA Nprintf field, configure the IP address of the PC which is on the same subnet as the ATA 186.
2. The port specified after the address must be **9001**.
3. At the DOS prompt on the PC, issue the **preserv.exe** program.

You can download the preserv.exe program from the Cisco Software Center (registered customers only) .

The preserv.exe program is included in the latest ATA 186 software release ZIP file.

Sample Debugs for Calls Made from the ATA 186

```
D:\Documents and Settings\sshafiqu\My Documents\voice\ata>prserv.exe
GK<-1: KPA-RRQ:300 sec
GK->1: RCF:TTL 300

!--- ATA was reset after the gatekeeper configuration was added.

WStop:0
Wed Feb 06 19:06:54 2002 Hello from 171.69.85.90(0)
Build 1109a: v2.12 ata186
Successfully Registered with the Gatekeeper
GK zone<gk2>172.16.13.12: 3000
GK zone:gk2
0x13e138 delayed RRQ: 48 ticks: 300
GK zone<gk2>172.16.13.12: 3001
GK zone:gk2
0x141e58 delayed RRQ: 56 ticks: 300
BMK : gk2
GK<-1: KPA-RRQ:300 sec
BMK : gk2
GK<-0: KPA-RRQ:300 sec
```

```
GK->1: RCF:TTL 300
GK->0: RCF:TTL 300
SCC->(0 0) <cmd 0>
3000 active @0xab45555a (GK @0xac100d0c)
```

!--- Call made from voice port 0.

```
[0]DTMF 1
[0]DTMF 2
[0]DTMF 3
[0]DTMF 4
[0]DTMF #
Calling 1234
SCC->(0 0) <cmd 16>
CLIP\
\SCC->(0 0) <cmd 2>
\<0 0> dial<1234>
GK<-0: ARQ: 0
GK->0: ACF:0:direct call
IRR in 240 sec
CallRasCallBack: 1 33e15eb 33e206b 33e39b0
Connect to <0xac100d28 1720>>..
>>>>>>>> TX CALLER ID : 0x1          0x80 6
Q931<-0:Setup:CRV 25006
Q931->0:Proceeding
Connect H245...
H245 TCP conn ac100d28 11006
CESE/MSDSE start:<0 0 0 0>
capSize = 3
H245->0:Cese
RemoteInputCap <15 5>
RemoteInputCap <15 4>
RemoteInputCap <15 1>
RemoteInputCap <4 11>
MODE FRAME : 11 2
RemoteAudioCap <4 10>
Capability set accepted
H245->0:MSD: <rn tt> = <0x269c 60>
H245->0:CeseAck
H245->0:MsdAck
h323.c 1837: cstate : 3
->H245<0> OLC
H245<-0:LcseOpen
set TX audio to G729/G729A 2 fpp
SetG723Mode: 2 0
H245->0:LcseOpen
H245->0:OLC mode 10
remote OpenLogicalReq G711/G729(10) : 2 fpp
OpenRtpRxPort(0,0x0,4000):14
RTP Rx Init: 0, 0
RTP->0:<0xab45555a 4000>
H245->0:LcseOpenAck
RTP<-0:<0xac100d28 17304>
[0]Enable encoder 18
RTP TX[0]:SSRC_ID = 4af964c0
RTP Tx Init: 0, 0
[0]DPKT 1st: 861812319 861812079, pt 18
Enable LEC adapt [0]=1
H323Dispatcher : 3 3
[0]Received pi=8 in q931
Q931->0:Progress
Q931->0:Connect
SCC:ev=12[0:0] 3 0
Q931->0:ReleaseComplete: reason 16, tone = 13
H245<-0:EndSessionCmd 1
0: Close RTPRX
```

```
write TCP err : 13 -33
[0:0]Rel LBRC Res
Q931<-*:ReleaseComplete

!--- ATA side hangs up the call.

write TCP err : 12 -33
GK<-0: DRQ:0

!--- Disconnect request sent by ATA.

SCC:ev=13[0:0] 4 0
[0:0]SCC: Disconnected
GK->0: DCF

!--- Disconnect confirm received.

SCC->(0 0) <cmd 1>
[0]MPT mode 0
```

No Dial Tone ATA Debug Example

Both voice ports need a unique E.164 address, otherwise the ATA receives a Reject from the gatekeeper. During this time, you will see the ATA 186 being registered with one voice port as an H.323 terminal, but there will be no dial tone.

```
K<-0: GRQ
BMK : gk2
GK->0: GCF:GK@0xac100d0c-1719
BMK : gk2
Secured RRQ
GK<-0: RRQ
GK->0:RRJ: reason 4
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Voice
Service Providers: Voice over IP
Voice & Video: Voice over IP
Voice & Video: IP Telephony
Voice & Video: IP Phone Services for End Users
Voice & Video: Unified Communications
Voice & Video: IP Phone Services for Developers
Voice & Video: General

Related Information

- **Cisco ATA 186 Basic Configuration**
- **Configuring and Troubleshooting an ATA 186 with a Cisco IOS Gateway**
- **Cisco High−Performance Gatekeeper – Configuring the Gatekeeper**

- **Configuring Voice over IP**
- **Voice Technology Support**
- **Voice and IP Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation – Cisco Systems**

Updated: Aug 06, 2007   Document ID: 19084